Securitatea Datelor

Laboratorul nr.5: Brute Force

Cuprins

[1. Definiție 3](#_Toc7506)

[2. Recomandare 3](#_Toc7507)

[3. Demonstrație atac Brute Force 3](#_Toc7508)

[3.1 Aplicații utilizate 3](#_Toc7509)

[3.2 Configurare aplicații 3](#_Toc7510)

# Definiție

Brute Force este un atac cibernetic care are scopul de a identifica credențialele unui utilizartor. în majoritatea cazelor folosesc dicționarele de parole, în realizarea acesor dicționare este important să cunoaște cât mai multe date despre țintă.

# Recomandare

Utilizați parole complexe. Ca o regulă generală, toate parolele asociate cu orice cont de utilizator ar trebui să posede cel puțin 10 caractere și să fie complexe, în sensul de a include caractere speciale, cifre, litere mici și litere mari;

# Demonstrație atac Brute Force

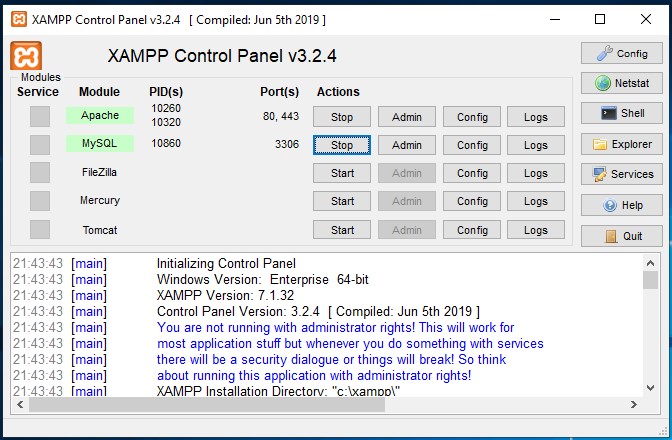
În laboratorul nr.4 se va exemplifica un atac de tipul Brute Force asupra aplicației pe care am învățat să o instalăm în laboratorul nr.1 (Damn Vulnerable Web Application – DVWA).

## Aplicații utilizate

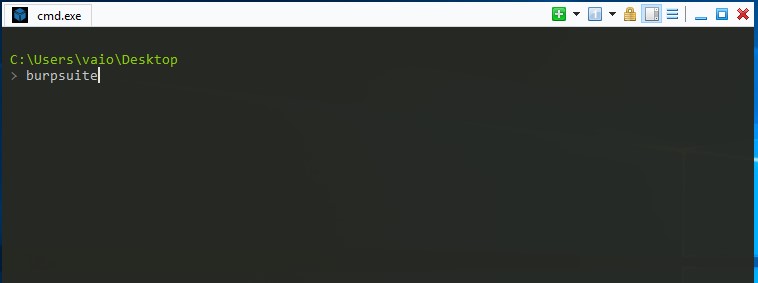
* Damn Vulnerable Web Application – (aplicația asupra căreia se va realiza atacul)
* BurpSuite (Utilitar specific atacurilor de tipul Brute Force – ( utilitar din Pentest Box)

## Configurare aplicații

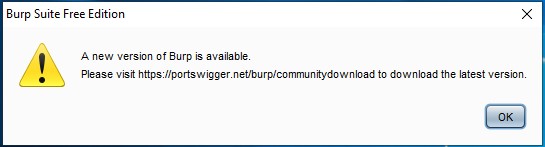
* Pasul 1. Pornim modulele Apache și MySQL din XAMPP (necesare aplicației DVWA).



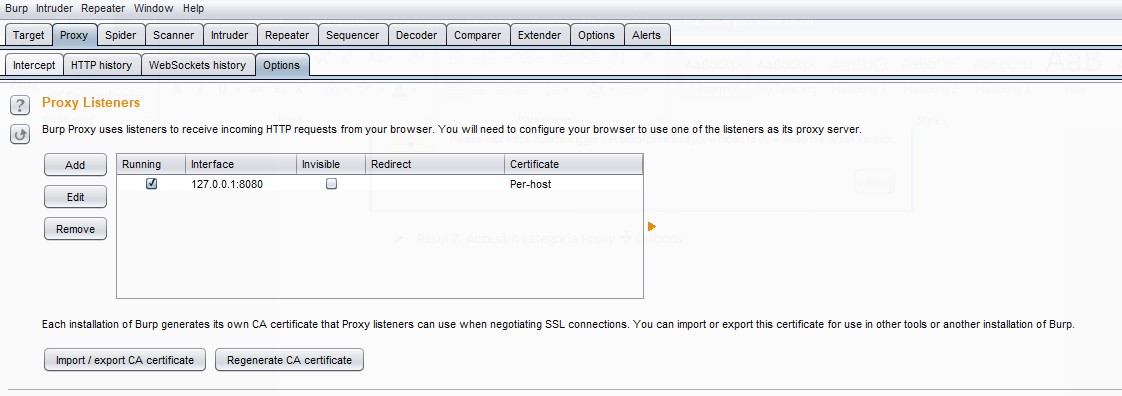
Pasul 2. Pornim aplicația BurpSuite din Pentest Box - scriem următoarea comandă în terminal:



* Pasul 3. La primirea mesajului din următoarea imagine apăsăm butonul OK



* Pasul 4. Accesăm categoria Proxy → Options



* Pasul 5. Verificăm dacă sunt următoarele setări
  + Running – bifat
  + Interface: 127.0.0.1:8080

Pasul 6. Istamlăm Mozilla Firefox versiunea 45.0



Link download:<https://www.filepuma.com/download/mozilla_firefox_64bit_45.0-10865/>

* Pasul 7. Accesăm aplicația dvwa cu browserul Mozilla Firefox <http://localhost/dvwa/login.php>

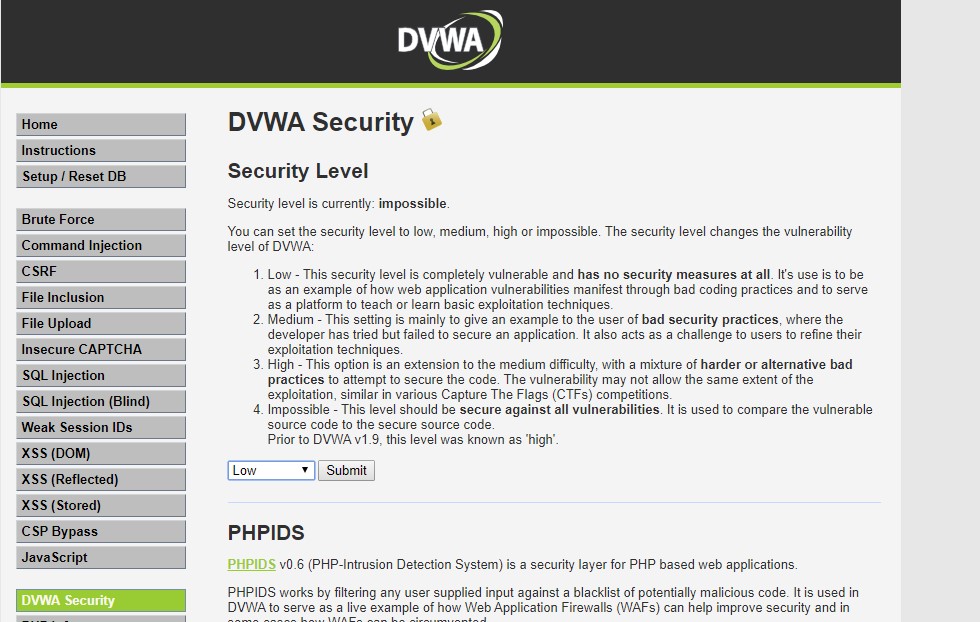


* Pasul 8. Ne autentificăm cu următoarele credențiale:

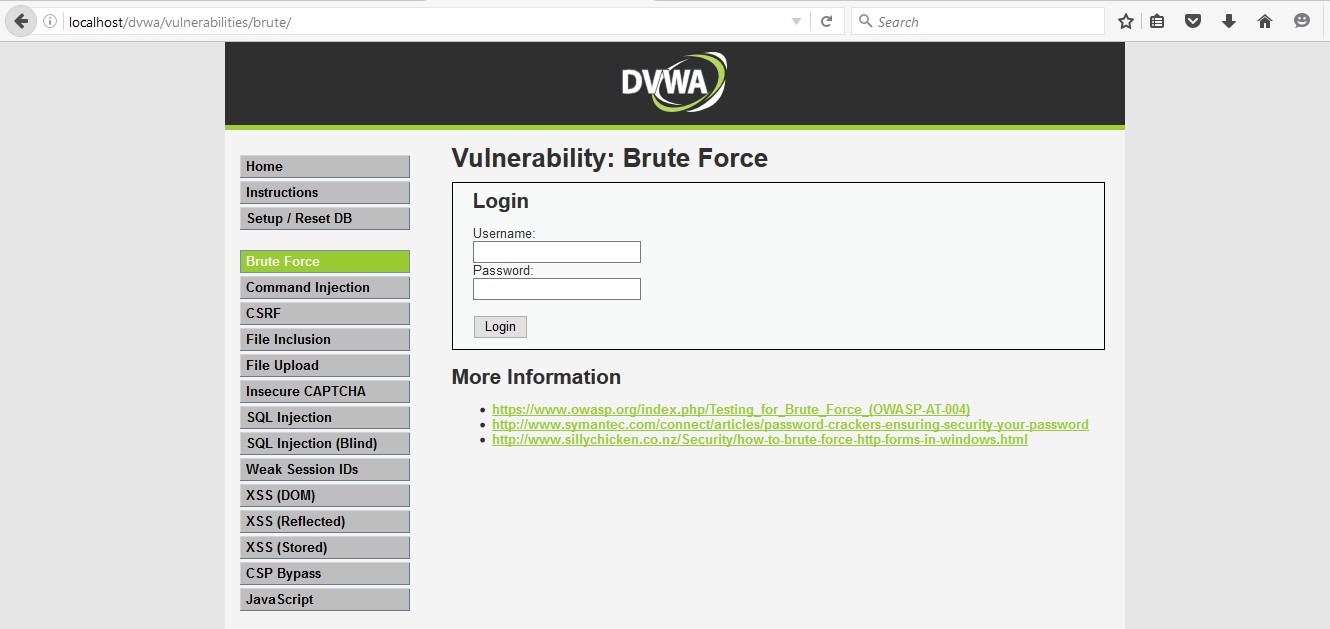
Username: admin

Passsword: password

Pasul 9. Din tab-ul din partea stângă accesăm categoria DVWA Security – setăm nivelul de securitate Low și apăsăm butonul Submit

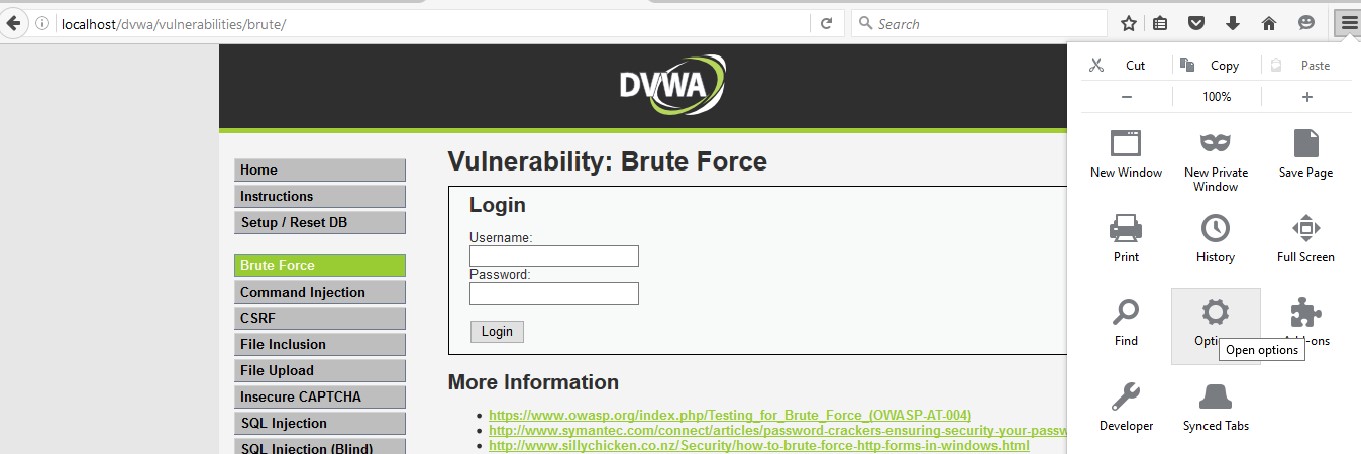


* Pasul 10. Accesăm categoria Brute Force

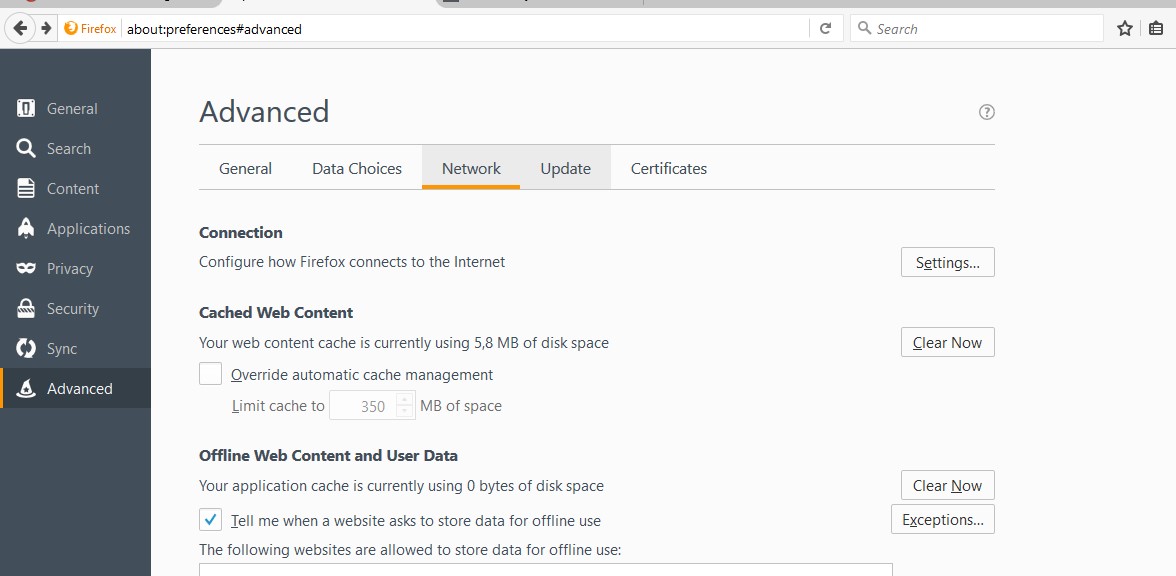


Pasul 11. Realizăm următoarele setări în browser

* + - Selectăm din Meniu categoria Options



* + - Din tab-ul din partea stângă selectăm Advanced → Network

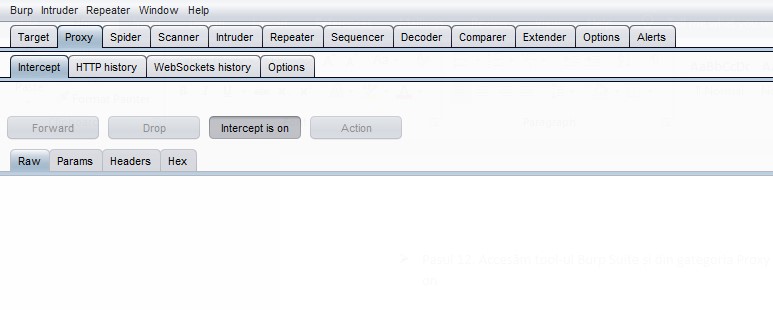


* + - Dăm click pe Settings și la Connection Settings facem următoarele setări:

o Bifăm Manual proxy configuration o HTTP Proxy: 127.0.0.1 o Port: 8080 o Bifăm Use this proxy server for all protocols o Click butonul OK

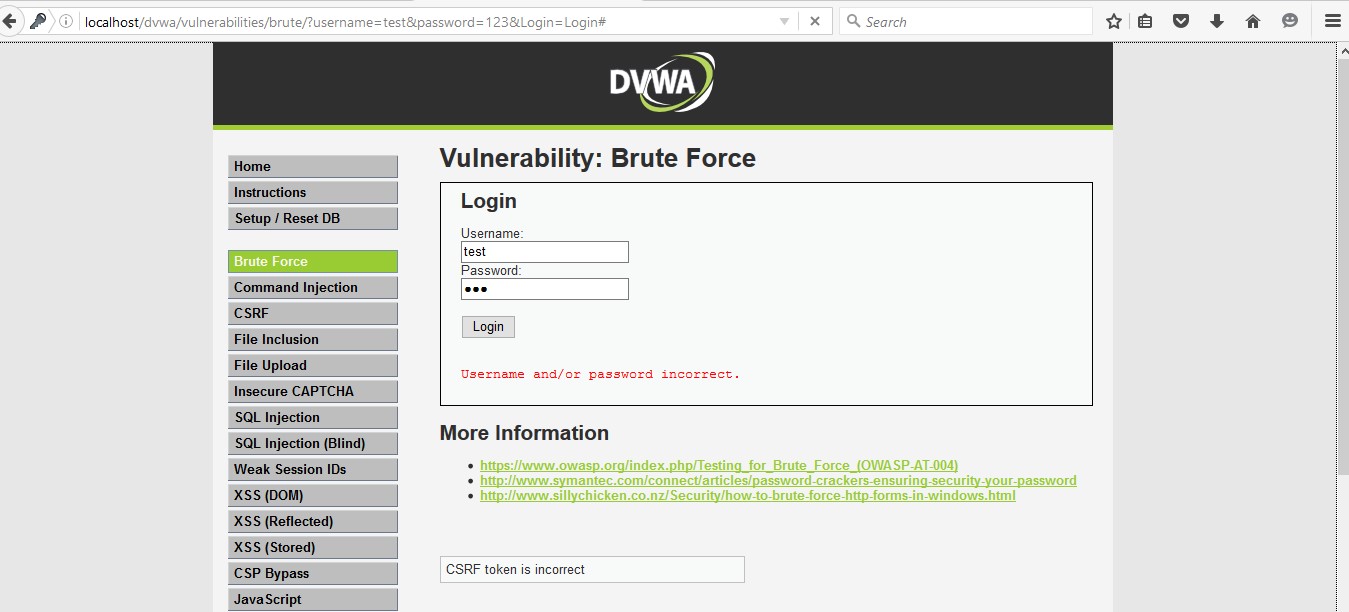


* Pasul 12. Accesăm tool-ul Burp Suite și din gategoria Proxy → Intercept setăm Intercept is on

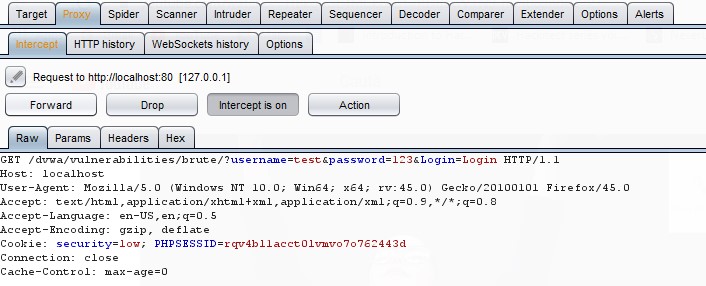


* Pasul 13. Accesăm browser-ul Mozilla (pasul 10[)http://localhost/dvwa/vulnerabilities/brute/](http://localhost/dvwa/vulnerabilities/brute/) și introducem:

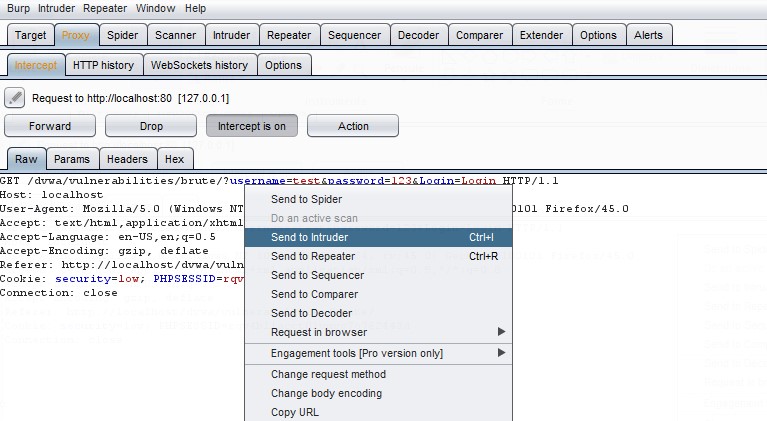
o username: test o Password: 123



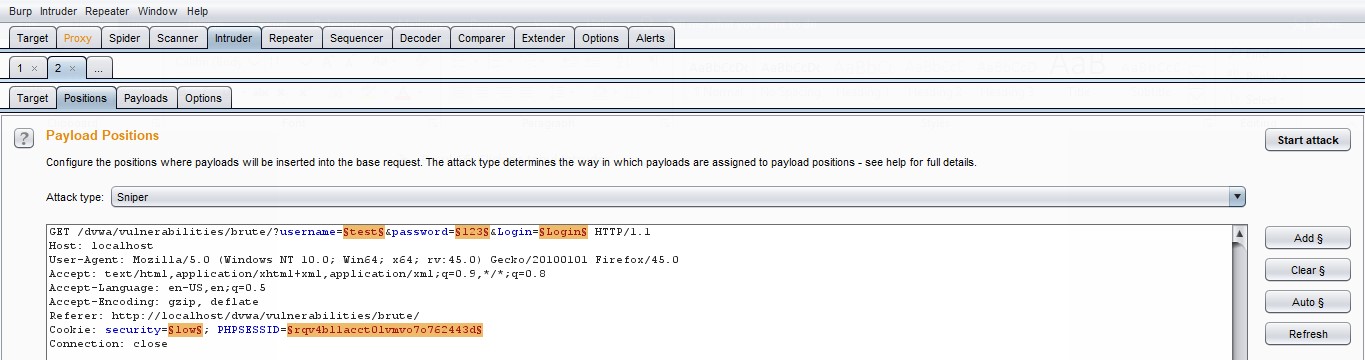
Pasul 14. Deschidem aplcația Burp Suite, în tabul Intercep din proxy a fost interceptat:



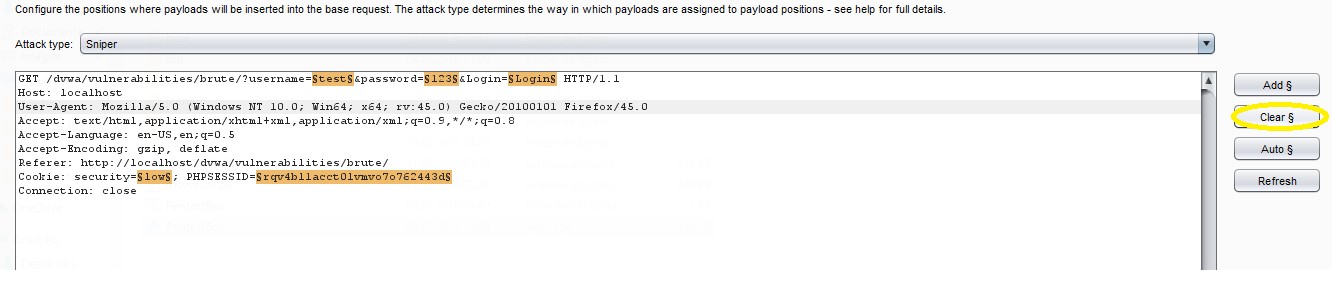
* Pasul 15. Click dreapta și selectăm Send to Intruder (sau CTRL+I)



Pasul 16. Click pe tabul Intruder



* Pasul 17. Din meniul din partea dreapta selectăm Clear §



* Pasul 18. Selectăm test și facem click pe Add §, la fel și pentru 123 ( pentru a selecta poziția de brutforce). Textul după modificari trebuie să arate astfel:

GET /dvwa/vulnerabilities/brute/?username=§test§&password=§123§&Login=Login HTTP/1.1

Host: localhost

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:45.0) Gecko/20100101 Firefox/45.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

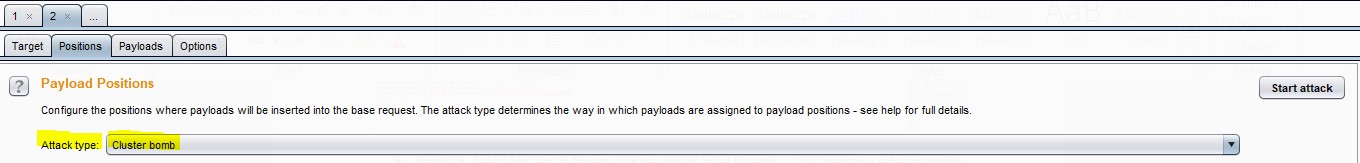
Accept-Encoding: gzip, deflate

Referer: http://localhost/dvwa/vulnerabilities/brute/

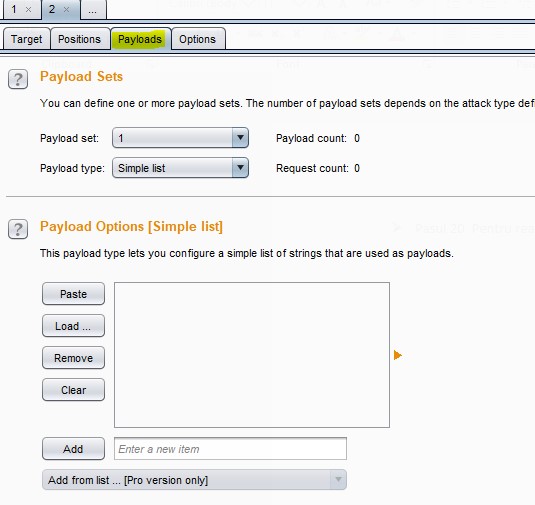
Cookie: security=low; PHPSESSID=rqv4bl1acct0lvmvo7o762443d

Connection: close

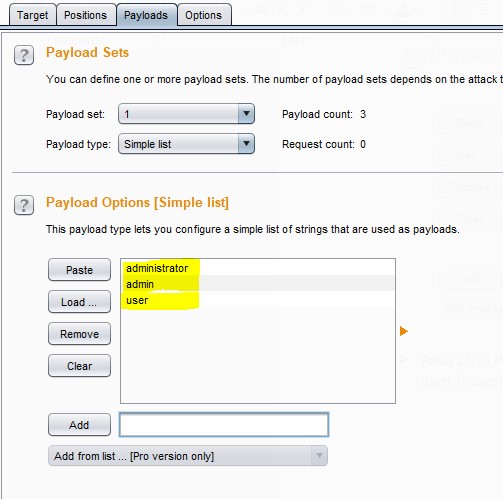
* Pasul 19. Selctăm tipul de atac, în cazul nostru este **Cluster bomb**



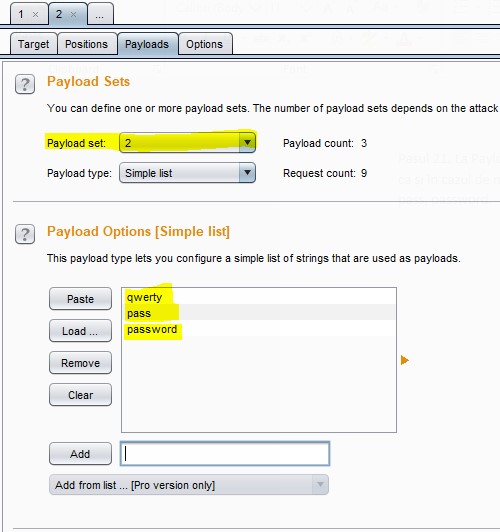
Pasul 20. Pentru realizarea dicționarului de parole accesăm categoria **Payloads**



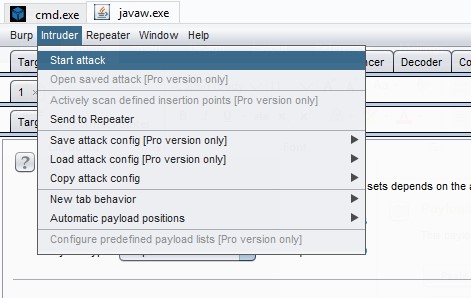
* Pasul 21. La Payload Options [Simple list] – adăugăm cuvinte pentru a forma dicționarul cu useri. În cazul nostru adăugăm: admin, administrator, user



Pasul 21. La Payload → Payload Sets – selectăm 2 pentru a realiza dicționarul cu parole, și la fel ca și în cazul de mai sus la Payload Options [Simple list] – adăugăm următoarele cuvinte: qwerty, pass, password.



* Pasul 22. Pornim Atacul din tabul Intruder din bara de sus (Start attack)



Userul și parola cu lungimea (Length) 4738 sunt cele corecte

